This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

**Usage guidelines**

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

**About Google Book Search**

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

Mathematics
QA
201
.M116m
B 470368

The University of Chicago

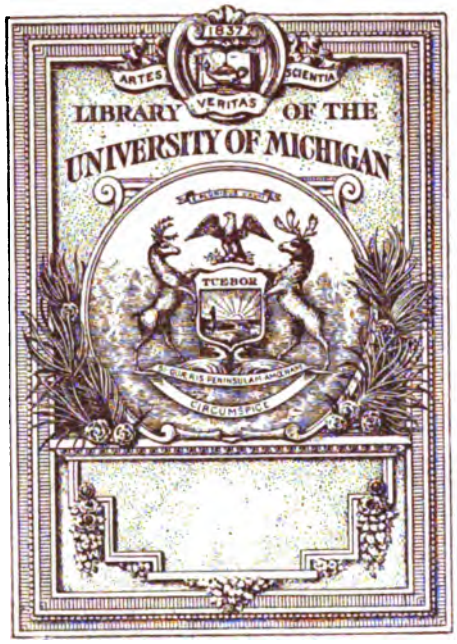
# MODULAR INVARIANTS OF A QUADRATIC FORM FOR A PRIME POWER MODULUS

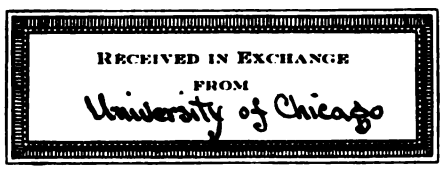
A DISSERTATION
SUBMITTED TO THE FACULTY
OF THE OGDEN GRADUATE SCHOOL OF SCIENCE
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
DEPARTMENT OF MATHEMATICS

BY
JAMES ELIJAH McATEE

A Private Edition, Distributed By
The University of Chicago Libraries
Chicago, Illinois

Reprinted from
AMERICAN JOURNAL OF MATHEMATICS
Vol. XLI, No. 3, July, 1919


1837
ARTES
VERITAS
SCIENTIA
LIBRARY OF THE
UNIVERSITY OF MICHIGAN
TUEBOR
CIRCUMSPICE


RECEIVED IN EXCHANGE
FROM
University of Chicago

MATHEMATICS
QA
201
.M116m

The University of Chicago

# MODULAR INVARIANTS OF A QUADRATIC FORM FOR A PRIME POWER MODULUS

A DISSERTATION
SUBMITTED TO THE FACULTY
OF THE OGDEN GRADUATE SCHOOL OF SCIENCE
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
DEPARTMENT OF MATHEMATICS

BY
JAMES ELIJAH McATEE

A Private Edition, Distributed By
The University of Chicago Libraries
Chicago, Illinois

Reprinted from
AMERICAN JOURNAL OF MATHEMATICS
Vol. XLI, No. 3, July, 1919

# *Modular Invariants of a Quadratic Form for a Prime Power Modulus.*

By J. E. McAtee.*

## Introduction.

We consider a quadratic form $q$ in $n$ variables whose coefficients are integers taken modulo $P^\lambda$, where $P$ is an odd prime. Two such forms are said to be equivalent modulo $P^\lambda$ if they become identically congruent under a linear homogeneous transformation whose coefficients are congruent to integers modulo $P^\lambda$ and their determinant is congruent to unity. All the forms equivalent to $q$ are said to form a class. A single-valued function $\phi$ of the coefficients of $q$ is an invariant of $q$ if it has the same value for all forms of the same class. In case the values taken by $\phi$ are integers which may be reduced modulo $P^\lambda$, the invariant is called modular. We obtain a complete invariantive classification of $n$-ary quadratic forms modulo $P^\lambda$ and construct modular invariants which completely characterize the classes. Professor Dickson† had treated the problem for the case $\lambda=1$, when the fundamental invariants are the determinant $D$ of $q$, the rank $r$ modulo $P$ of $D$, and $A_r$, to which the invariant $A_{\bar{R}_0}(D)$ of § 4 reduces for $\lambda=1$.

In his investigation of the number of sets of solutions of the congruence $q\equiv c \pmod{P^\lambda}$, C. Jordan‡ obtained from $q$ by a seriatim process of reduction the canonical form

$$P^{e_1}(A_1x_1^2+\ldots+A_sx_s^2)+P^{e_2}(A_{s+1}x_{s+1}^2+\ldots+A_tx_t^2)+P^{e_3}()+\ldots,$$

but gave no explicit method to deduce à priori from $q$ the number of terms in each parenthesis or the values of $e_1, e_2 \ldots$. This is accomplished by the present invariants.

The second part of the paper is devoted to the polynomial modular invariants of a binary quadratic form modulo $P^\lambda$, in particular to the determination of a fundamental system of such invariants modulo 4.

---

* Dr. McAtee died at Urbana, Ill., Dec. 2, 1918. The proof-sheets were compared with both the final and an initial draft of the thesis. In § 7, an inadequate proof of Theorem 1 has been replaced by the present shorter proof, while the easy proofs of some other facts have been omitted. The proof of formula (3) of § 1 has been suppressed, as it was entirely similar to that cited. L. E. Dickson.

† Madison Colloquium Lectures, 1913, Ch. 1; *Trans. Amer. Math. Soc.*, Vol. X (1909), p. 123.

‡ *Jour. de Math.*, (2), Vol. XVII (1872), pp. 368–402. Cf. Bachmann, "Die Arith. der Quadratischen Formen" (1898), p. 434.

344440

## I. INVARIANTS OF THE $n$-ARY QUADRATIC FORM MODULO $P^\lambda$.

1. *Canonical Forms and Classes.*—Consider the form

$$q_n=\sum_{i,j=1}^{n} a_{ij}x_ix_j \qquad (a_{ij}=a_{ji}), \tag{1}$$

where the $a_{ij}$ are integers taken modulo $P^\lambda$, where $P$ is an odd prime. If every $a_{ij}$ is divisible by $P^\lambda$, the form (1) is said to constitute the class $C_0$. In the contrary case, let $e_1$ be the exponent of the highest power of $P$ that divides every $a_{ij}$, and write

$$q_n=P^{e_1}\sum_{i,j=1}^{n} A_{ij}^{(1)}x_ix_j, \qquad D=|A_{ij}^{(1)}|. \tag{2}$$

First, let the determinant $D$ be prime to $P$. Since there exists a primitive root of $P^\lambda$, it follows as in the Madison Colloquium Lectures, pp. 6, 7, that $q_n$ can be transformed into

$$P^{e_1}[x_1^2+\ldots.+x_{n-1}^2+Dx_n^2] \tag{3}$$

by a linear transformation with integral coefficients of determinant unity modulo $P^\lambda$.

Second, let $D$ be divisible by $P$, and $r_1$ its rank modulo $P$. As on p. 9 of the Lectures cited, we may assume that

$$M_{r_1}=|A_{ij}^{(1)}|\not\equiv 0 \pmod P \qquad (i,j=1,\ldots.,r_1),$$

and show* that $q_n$ can be transformed into

$$P^{e_1}[\sum_{i,j=1}^{n-1} A_{ij}^{(1)}x_ix_j+2\sum_{j=r_1+1}^{n-1} B_{jn}^{(1)}x_jx_n+B_{nn}^{(1)}x_n^2],$$

where

$$B_{jn}^{(1)}\equiv\begin{vmatrix} A_{11}^{(1)}\ldots.A_{1r_1}^{(1)} & A_{1n}^{(1)} \\ \ldots\ldots\ldots\ldots & \\ A_{r_11}^{(1)}\ldots.A_{r_1r_1}^{(1)} & A_{r_1n}^{(1)} \\ A_{j1}^{(1)}\ldots.A_{jr_1}^{(1)} & A_{jn}^{(1)} \end{vmatrix} M_{r_1}^{-1} \qquad (j=r_1+1,\ldots.,n)$$

is congruent to an integer modulo $P^\lambda$ and is divisible by $P$. Repetitions of this process give

$$P^{e_1}[\sum_{i,j=1}^{r_1} A_{ij}^{(1)}x_ix_j+\sum_{i,j=r_1+1}^{n} B_{ij}^{(1)}x_ix_j], \tag{4}$$

where

$$B_{ij}^{(1)}\equiv\begin{vmatrix} A_{11}^{(1)}\ldots.A_{1r_1}^{(1)} & A_{1j}^{(1)} \\ \ldots\ldots\ldots\ldots & \\ A_{r_11}^{(1)}\ldots.A_{r_1r_1}^{(1)} & A_{r_1j}^{(1)} \\ A_{i1}^{(1)}\ldots.A_{ir_1}^{(1)} & A_{ij}^{(1)} \end{vmatrix} M_{r_1}^{-1}$$

is congruent to an integer modulo $P^\lambda$ and is divisible by $P$. If now all the $P^{e_1}B_{ij}^{(1)}$ are zero modulo $P^\lambda$, we have $q_n$ replaced by

$$P^{e_1}\sum_{i,j=1}^{r_1} A_{ij}^{(1)}x_ix_j.$$

---

* Using $P^{e_1}B_{jm}\equiv 0 \pmod{P^\lambda}$ in place of $B_{jm}\equiv 0 \pmod P$.

In the contrary case let $e_2$ denote the highest power of $P$ that divides all the $P^{e_1}B_{ij}^{(1)}$ $(e_1<e_2<\lambda)$. Then we have (4) expressed in the form

$$P^{e_1}\sum_{i,\,j=1}^{r_1}A_{ij}^{(1)}x_ix_j+P^{e_2}\sum_{i,\,j=r_1+1}^{n}A_{ij}^{(2)}x_ix_j, \tag{5}$$

where at least one of the $A_{ij}^{(2)}$ is prime to $P$. The question now arises as to whether a different choice of $M_{r_1}$ might not lead to a set of $B_{ij}^{(1)}$ that would give a different $e_2$. To answer this we note that, since $M_{r_1}$ is prime to $P$ and hence is congruent to a power $\rho^m$ of a primitive root $\rho$ of $P^\lambda$, we can transform (5) into

$$P^{e_1}[x_1^2+\ldots.+x_{r_1-1}^2+\rho^m x_{r_1}^2]+P^{e_2}\sum_{i,\,j=r_1+1}^{n}A_{ij}^{(2)}x_ix_j.$$

By applying a transformation of the type

$$x_{r_1}=\rho^{-k}x'_{r_1},\quad x_n=\rho^k x'_n,$$

we obtain one of the forms

$$\left.\begin{aligned}&P^{e_1}[x_1^2+\ldots.+x_{r_1}^2]+P^{e_2}q\quad (q\text{ free of }x_1,\ldots.,x_{r_1}),\\&P^{e_1}[x_1^2+\ldots.+x_{r_1-1}^2+\rho x_{r_1}^2]+P^{e_2}q_\rho\quad (q_\rho\text{ free of }x_1,\ldots.,x_{r_1}).\end{aligned}\right\} \tag{6}$$

If we had chosen $M'_{r_1}$ instead of $M_{r_1}$, we would have obtained from (2) one of

$$\left.\begin{aligned}&P^{e_1}[y_1^2+\ldots.+y_{r_1}^2]+P^{e'_2}q'\quad (q'\text{ free of }y_1,\ldots.,y_{r_1}),\\&P^{e_1}[y_1^2+\ldots.+y_{r_1-1}^2+\rho y_{r_1}^2]+P^{e'_2}q'_\rho\quad (q'_\rho\text{ free of }y_1,\ldots.,y_{r_1}).\end{aligned}\right\} \tag{7}$$

Since * $\qquad x_1^2+\ldots.+x_{r_1}^2$ and $y_1^2+\ldots.+y_{r_1-1}^2+\rho y_{r_1}^2$

are not equivalent modulo $P$, it is evident that if we obtain $(6_1)$ by the use of $M_{r_1}$ we must obtain $(7_1)$ by the use of $M'_{r_1}$. Similarly, if we obtain $(6_2)$ by the use $M_{r_1}$ we must obtain $(7_2)$ by the use of $M'_{r_1}$. For definiteness, suppose that we obtain $(6_1)$ and $(7_1)$ and that $e_2<e'_2$. Then the forms

$$P^{e_1}(x_1^2+\ldots.+x_{r_1}^2)+P^{e_2}q\quad\text{and}\quad P^{e_1}(y_1^2+\ldots.+y_{r_1}^2)$$

are transformable into each other modulo $P^{e'_2}$, whenever the forms

$$x_1^2+\ldots.+x_{r_1}^2+P^kq\quad\text{and}\quad y_1^2+\ldots.+y_{r_1}^2$$

are transformable into each other modulo $P^l$, where $l=e'_2-e_1$ and $k=e_2-e_1$. Let the second of these be transformed into the first by

$$T:\ y_i\equiv\sum_{j=1}^{n}c_{ij}x_j\pmod{P^l}.$$

Employing partial derivatives with respect to $x_i$, we have

$$S:\left\{\begin{aligned}&x_1\equiv c_{11}y_1+\ldots.+c_{r_11}y_{r_1},\\&\ldots\ldots\ldots\ldots\ldots\ldots\\&x_{r_1}\equiv c_{1r_1}y_1+\ldots.+c_{r_1r_1}y_{r_1}\end{aligned}\right\}\pmod{P^l}.$$

* L. E. Dickson, The Madison Colloquium Lectures, 1913, p. 8.

The inverse of $S$ gives $y_i$ $(i=1, \ldots, r_1)$ congruent to linear homogeneous functions of $x_1, \ldots, x_{r_1}$ modulo $P^l$. Hence, if $(6_1)$ and $(7_1)$ are equivalent modulo $P^\lambda$, $P^k q \equiv 0 \pmod{P^l}$ for all integral values of $x_{r_1+1}, \ldots, x_n$. Since at least one of the coefficients in $q$ is prime to $P$, this implies that $k \geqq l$, *i. e.*, that $e_2 \geqq e_2'$. Similarly, $e_2'$ can not be less than $e_2$. Therefore, the choice of the principal minor of $|A_{ij}^{(1)}|$ that is prime to $P$ is immaterial so far as the value of $e_2$ is concerned. Consider now the two forms

$$Q = x_1^2 + \ldots + x_{r_1}^2 + P^l q, \quad Q' = y_1^2 + \ldots + y_{r_1}^2 + P^l q'.$$

Let $Q$ and $Q'$ be equivalent modulo $P^{\lambda - e_1}$ and let

$$T: \; y_i \equiv \sum_{j=1}^{n} c_{ij} x_j \pmod{P^{\lambda - e_1}} \qquad (i=1, \ldots, n)$$

transform $Q'$ into $Q$ modulo $P^{\lambda - e_1}$, where $|c_{ij}| \not\equiv 0 \pmod{P}$. Then we have

$$S: \left\{ \begin{array}{l} \dfrac{\partial Q}{\partial x_1} = 2x_1 \equiv 2c_{11}y_1 + \ldots + 2c_{r_1 1}y_{r_1} + P^l \dfrac{\partial q'}{\partial x_1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \dfrac{\partial Q}{\partial x_{r_1}} = 2x_{r_1} \equiv 2c_{1 r_1}y_1 + \ldots + 2c_{r_1 r_1}y_{r_1} + P^l \dfrac{\partial q'}{\partial x_{r_1}} \end{array} \right\} \pmod{P^{\lambda - e_1}},$$

which shows that $|c_{ij}|$ $(i, j=1, \ldots, r_1)$ is prime to $P$. The inverse of $S$ gives $y_1, \ldots, y_{r_1}$ expressed as linear homogeneous functions of $x_1, \ldots, x_{r_1}$, $y_{r_1+1}, \ldots, y_n$. Moreover, the coefficients of $y_{r_1+1}, \ldots, y_n$ in these functions are divisible by $P^l$. Hence $T$ is expressible in the form

$$y_i \equiv \sum_{j=1}^{r_1} c_{ij}x_j + P^l \sum_{j=r_1+1}^{n} c'_{ij}y_j \pmod{P^{\lambda - e_1}} \qquad (i=1, \ldots, r_1),$$

$$y_i \equiv \sum_{j=1}^{n} c_{ij}x_j \pmod{P^{\lambda - e_1}} \qquad (i=r_1+1, \ldots, n).$$

Subjecting $Q'$ to this transformation, we have

$$\phi(x_1, \ldots, x_{r_1}) + P^l \theta(x_1, \ldots, x_n).$$

Since, by hypothesis, $T$ transforms $Q'$ into $Q$ modulo $P^{\lambda - e_1}$, the terms in $\theta$ involving $x_1, \ldots, x_{r_1}$ must vanish modulo $P^{\lambda - e_1}$, and we have

$$\phi \equiv x_1^2 + \ldots + x_{r_1}^2 \pmod{P^{\lambda - e_1}}.$$

From this we see that the equivalence of $(6_1)$ and $(7_1)$ modulo $P^\lambda$ implies the equivalence of $P^{e_2}q$ and $P^{e_2}q'$. Similarly, for the equivalence of $(6_2)$ and $(7_2)$. This shows that in the method of reduction of a quadratic form to the canonical form (8) or (9) modulo $P^\lambda$, it is immaterial whether we effect it by employing principal minors or by a seriatim process as was done by Jordan in a similar case.* This seriatim process is given in the argument leading up to (3).

---

* *Journal de Mathématiques*, Ser. 2, Vol. XVII (1872), pp. 368–375.

Repetitions of the arguments leading to (5) and (6) show that there exists a linear homogeneous transformation of determinant unity modulo $P^\lambda$ under which, when $|P^{-e_1}a_{ij}|$ is divisible by $P$, the form (1) becomes

$$P^{e_1}[x_1^2+\ldots.+x_{r_1-1}^2+\rho^{m_1}x_{r_1}^2]+P^{e_2}[x_{r_1+1}^2+\ldots.+x_{r_1+r_2-1}^2+\rho^{m_2}x_{r_1+r_2}] \\ +\ldots.+P^{e_k}[x_{r_1+r_2+\ldots.+r_{k-1}+1}^2+\ldots.+x_{r_1+\ldots.+r_k-1}^2+\rho^{m_k}x_{r_1+\ldots.+r_k}^2] \quad (8)$$

if $r_1+r_2+\ldots.+r_k<n$, or

$$P^{e_1}[x_1^2+\ldots.+x_{r_1-1}^2+\rho^{m_1}x_{r_1}^2]+P^{e_2}[x_{r_1+1}^2+\ldots.+x_{r_1+r_2-1}^2+\rho^{m_2}x_{r_1+r_2}^2] \\ +\ldots.+P^{e_k}[x_{r_1+\ldots.+r_{k-1}+1}^2+\ldots.+x_{n-1}^2+P^{-\sum_{i=1}^{k}r_ie_i}\rho^{-\sum_{i=1}^{k-1}m_i}Dx_n^2] \quad (9)$$

if $r_1+r_2+\ldots.+r_k=n$, where $m_i=0$ or $1$ [$i=1, \ldots., k$ in (8); $i=1, \ldots., k-1$ in (9)], $D=|a_{ij}|$ and $r_s$ is the rank modulo $P$ of the determinant

$$|A_{ij}^{(s)}| \ (i, j=r_1+r_2+\ldots.+r_{s-1}+1, \ldots., n).$$

$A_{ij}^{(s)}=P^{-e_s}B_{ij}^{(s-1)}$, where the $B_{ij}^{(s-1)}$ are found from the $A_{ij}^{(s-1)}$ in the same way that the $B_{ij}^{(1)}$ were found from $A_{ij}^{(1)}$ in (4). Therefore, when not all the $a_{ij}$ are zero modulo $P^\lambda$, we have the canonical forms (3), (8), (9), and from the work above it is evident that two forms are equivalent modulo $P^\lambda$, if and only if they have the same canonical form. Since (3) is a special case of (9) with $k=1$, *i. e.*, $r_1=n$, we need consider only the canonical forms (8), (9) and the vanishing form where $a_{ij}\equiv 0 \pmod{P^\lambda}$ $(i, j=1, \ldots., n)$. Moreover, since two forms are equivalent modulo $P^\lambda$ if and only if they have the same canonical form, we have the classes $C_0$ and $Ce_im_iR_k$, defined by a canonical form of type (8) with $n>R_k=r_1+\ldots.+r_k$; $Ce_im_jnD$, defined by a canonical form of type (9) with $n=R_k$, for $i=1, \ldots., k$; $j=1, \ldots., k-1$; $e_i<\lambda$.

2. *Elementary Exponents and Ranks.*—Consider the symmetric determinant $D=|a_{ij}|$ $(i, j=1, \ldots., n)$, where the elements are integers. If $P^{\alpha_i}$ is the highest power of $P$ that divides all the $i$-rowed minors of $D$, then $\alpha_i$ is unchanged when $D$ is pre-multiplied or post-multiplied by an $n$-th order determinant whose elements are integers and whose value is unity.* Frobenius called the $P^{e_i}$ $(e_i=\alpha_i-\alpha_{i-1}, e_1=\alpha_1)$ the elementary invariants of $D$ with respect to $P$. We shall call the $e_i$ the elementary exponents of $D$ with respect to $P$, or simply the elementary exponents of $D$. Note for later use that† $e_i$ is a monotonically increasing function of $i$. Let $P^{e_1}$ be the highest power of $P$ that divides all the $a_{ij}$ and consider the case when $e_1<\lambda$. Let the rank modulo $P$ of

* Stephen Smith, *Phil. Trans.*, Vol. CLI, § 12, p. 311. Bachmann's *Zahlentheorie*, Vol. IV. Frobenius, *Berlin Sitzungsberichte* (1894), Pt. I, p. 31. These properties hold if $D$ is not symmetric, but our interest lies in the theorem as given.

† Frobenius, *loc. cit.* Also seen from this section.

the determinant $|A_{ij}| = |P^{-e_1}a_{ij}|$ be $r_1$, $0<r_1<n$. Then there exists* a principal minor $M_{r_1}$ of $|A_{ij}|$ of order $r_1$ that is prime to $P$. By multiplying $D$ by properly chosen unit determinants we may assume that

$$|A_{ij}| = M_{r_1} \not\equiv 0 \pmod{P} \qquad (i, j = 1, \ldots, r_1).$$

Consider the unit $n$-rowed determinant $d^{(1)} = |d_{st}^{(1)}|$ in which each element is zero except

$$d_{st}^{(1)} = 1 \text{ when } s = t, \quad d_{r_1+1,\,t}^{(1)} \equiv -\frac{A_{1,\,r_1+1}\bar{A}_{1t}}{M_{r_1}} \pmod{P^\lambda} \qquad (t = 1, \ldots, r_1),$$

where $\bar{A}_{ij}$ denotes the cofactor of $A_{ij}$ in $M_{r_1}$. If we pre-multiply $D$ by $d^{(1)}$ we have, upon denoting the resulting elements by $b_{ij}^{(1)}$,

$$b_{1,\,r_1+1}^{(1)} \equiv a_{1,\,r_1+1} - \frac{a_{1,\,r_1+1}}{M_{r_1}} \sum_{i=1}^{r_1} A_{1i}\bar{A}_{1i} \equiv 0 \pmod{P^\lambda},$$

$$b_{k,\,r_1+1}^{(1)} \equiv a_{k,\,r_1+1} - \frac{a_{1,\,r_1+1}}{M_{r_1}} \sum_{i=1}^{r_1} A_{ki}\bar{A}_{1i} \pmod{P^\lambda} \qquad (k \neq 1).$$

Hence

$$b_{k,\,r_1+1}^{(1)} \equiv a_{k,\,r_1+1} \pmod{P^\lambda} \qquad (1 < k \leq r_1),$$

$$b_{k,\,r_1+1}^{(1)} \equiv \frac{P^{e_1}}{M_{r_1}} [A_{k,\,r_1+1}M_{r_1} - A_{1,\,r_1+1}M_{r_1 1}^{(k)}] \qquad (k > r_1),$$

where $M_{r_1 1}^{(k)}$ denotes the determinant formed from $M_{r_1}$ by replacing its first row or column by the corresponding elements of the $k$-th row or column of $|A_{ij}|$ $(i, j = 1, \ldots, n)$. All other elements of $D$ are unchanged. If we now pre-multiply this resulting determinant by $d^{(2)} = |d_{st}^{(2)}|$, where $s, t = 1, \ldots, n$, and every element is zero except

$$d_{st}^{(2)} = 1 \text{ when } s = t; \quad d_{r_1+1,\,t}^{(2)} \equiv -\frac{A_{2,\,r_1+1}\bar{A}_{2t}}{M_{r_1}} \qquad (t = 1, \ldots, r_1),$$

we have

$$b_{1,\,r_1+1}^{(2)} \equiv b_{2,\,r_1+1}^{(2)} \equiv 0 \pmod{P^\lambda}, \quad b_{k,\,r_1+1}^{(2)} \equiv a_{k,\,r_1+1} \qquad (k = 3, 4, \ldots, r_1),$$

$$b_{k,\,r_1+1}^{(2)} \equiv \frac{P^{e_1}}{M_{r_1}} [A_{k,\,r_1+1}M_{r_1} - A_{1,\,r_1+1}M_{r_1 1}^{(k)} - A_{2,\,r_1+1}M_{r_1 2}^{(k)}] \pmod{P} \quad (k > r_1).$$

All other elements are again unchanged. Continuing this process, we ultimately obtain from $D$ a determinant having its first $r_1$ elements in the $(r_1+1)$-th row zero modulo $P^\lambda$ and the $k$-th element of this row $(k > r_1)$ is

$$P^{e_1}B_{k,\,r_1+1}^{(1)} \equiv \begin{vmatrix} A_{11} & \ldots . A_{1r_1} & A_{1k} \\ \ldots & \ldots\ldots & \ldots \\ A_{r_1 1} & \ldots . A_{r_1 r_1} & A_{r_1 k} \\ A_{r_1+1,\,1} & \ldots . A_{r_1+1,\,r_1} & A_{r_1+1,\,k} \end{vmatrix} P^{e_1}M_{r_1}^{-1} \pmod{P^\lambda}.$$

* L. E. Dickson, *Annals of Mathematics*, Ser. 2, Vol. XV (1913), pp. 27, 28.

$B^{(1)}_{k,r_1+1}$ is divisible by $P(r_1<k\leqq n)$, since $r_1$ is the rank modulo $P$ of the determinant $|A_{ij}|$ $(i, j=1, \ldots, n)$. All the elements of $D$ in any other row are unchanged. Operating similarly upon the $(r_1+2)$-th, ...., $n$-th row of this determinant and then post-multiplying by a properly chosen unit determinant, we ultimately obtain from $D$

$$D^{(1)}\equiv\begin{vmatrix} A & O \\ O & B \end{vmatrix} \pmod{P^\lambda}, \quad A=\begin{pmatrix} a_{11} \ldots . a_{1r_1} \\ \ldots\ldots\ldots \\ a_{r_11} \ldots . a_{r_1r_1} \end{pmatrix}, \quad B=\begin{pmatrix} P^{e_1}B^{(1)}_{r_1+1r_1+1} \ldots . P^{e_1}B^{(1)}_{r_1+1n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ P^{e_1}B^{(1)}_{nr_1+1} \ldots . P^{e_1}B^{(1)}_{nn} \end{pmatrix},$$

where $O$ is a matrix all of whose elements are zero.

Here $B^{(1)}_{ij}$ $(i, j=r_1+1, \ldots, n)$ is divisible by $P$. To determine the highest power of $P$ that divides all the $P^{e_1}B^{(1)}_{ij}$, let $P^{e'_2}$ denote the highest power of $P$ that divides all the $(r_1+1)$-rowed minors of $D$. Then $P^{e'_2}$ is the highest power of $P$ that divides all the $(r_1+1)$-rowed minors of $D^{(1)}$. Then evidently $P^{e'_2-e_1r_1}$ is the highest power of $P$ that divides all the $P^{e_1}B^{(1)}_{ij}$ of $D^{(1)}$. Let $e_2=e'_2-r_1e_1$. Then $e_2$ is the $(r_1+1)$-th elementary exponent of $D$. We shall call $r_1$ the first elementary rank of $D$ with respect to $P$. Consider the case when $e_2<\lambda$. Let $r_2$ be the rank modulo $P$ of the determinant

$$|P^{-(e_2-e_1)}B^{(1)}_{ij}| \qquad (i, j=r_1+1, \ldots . n).$$

Since there is a principal minor of this determinant of order $r_2$ that is prime to $P$, we may operate on this determinant as we did on $D$ above. Moreover, considering this determinant as it stands in $D^{(1)}$, we see that this operation would leave the first $r_1$ rows and columns of $D^{(1)}$ unaltered. Hence we would have

$$D^{(2)}\equiv\begin{vmatrix} A & O & O \\ O & B^{(1)} & O \\ O & O & C \end{vmatrix} \pmod{P^\lambda},$$

$$B^{(1)}=\begin{pmatrix} P^{e_1}B^{(1)}_{r_1+1, r_1+1} \ldots . P^{e_1}B^{(1)}_{r_1+1, r_1+r_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ P^{e_1}B^{(1)}_{r_1+r_2, r_1+1} \ldots . P^{e_1}B^{(1)}_{r_1+r_2, r_1+r_2} \end{pmatrix}, \quad C=\begin{pmatrix} P^{e_3}B^{(2)}_{r_1+r_2+1, r_1+r_2+1} \ldots . P^{e_3}B^{(2)}_{r_1+r_2+1, n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P^{e_3}B^{(2)}_{n, r_1+r_2+1} \ldots\ldots . P^{e_3}B^{(2)}_{n, n} \end{pmatrix}.$$

Let $P^{e'_3}$ be the highest power of $P$ that divides all the $(r_1+r_2+1)$-rowed minors of $D$. Then $e'_3-r_1e_1-r_2e_2=e_3$ is the highest power of $P$ that divides all the $P^{e_3}B^{(2)}_{ij}$ of $D^{(2)}$. Evidently we may continue this process until all the new elements are zero modulo $P^\lambda$, or until $\Sigma r_i=n$. At any stage, say the $t$-th, $e_t$ and $r_t$ are determined by the preceding. In fact

$$e_t=e'_t-\sum_{i=1}^{t-1} r_ie_i,$$

where $e'_t$ is the highest power of $P$ that divides all the $(r_1+r_2+\ldots .+r_{t-1}+1)$-rowed minors of $D$, and $r_t$ is an integer such that $E=r_1e_1+\ldots .+r_te_t$ is the

exponent of the highest power of $P$ that divides all the $(r_1+r_2+\ldots+r_i)$-rowed minors of $D$ while all the $(r_1+\ldots+r_i+1)$-rowed minors are divisible by a higher power of $P$ than $P^{E+e_i}$. We shall refer to these $r_i$ as the elementary ranks of $D$ with respect to $P$.

*Definition.* The determinant $D$ shall be said to be of rank $R$ modulo $P^\lambda$ if the $R$-th elementary exponent of $D$ with respect to $P$ is less than $\lambda$, while the $(R+1)$-th elementary exponent of $D$ is $\geqq\lambda$.

From this definition it follows that the rank of $D$ modulo $P^\lambda$ is an invariant under multiplication of $D$ by unit determinants and that under such multiplication $D$ becomes

$$D^{(k)}\equiv\begin{vmatrix} A & 0 & 0\ldots.0 & 0 & 0\ldots. \\ 0 & B^{(1)} & 0\ldots.0 & 0 & 0\ldots. \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & & \\ 0 & 0 & 0\ldots.0 & B^{(k)} & 0\ldots. \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & & \end{vmatrix} \pmod{P^\lambda},$$

$$B^{(k)}=\begin{pmatrix} P^{e_k}B^{(k)}_{R_k+1,\,R_k+1}\ldots.P^{e_k}B^{(k)}_{R_k+1,\,R_{k+1}} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ P^{e_k}B^{(k)}_{R_{k+1},\,R_k+1}\ldots.P^{e_k}B^{(k)}_{R_{k+1},\,R_{k+1}} \end{pmatrix},$$

where $R_i=r_1+\ldots+r_i$, and $R_k$ is the rank of $D$ modulo $P^\lambda$. The $e_1, e_2, \ldots, e_k$ are the distinct elementary exponents of $D$ that are less than $\lambda$ arranged in the order of increasing magnitude. From these considerations it follows that if the rank modulo $P^\lambda$ of a symmetric determinant $D$ is $R>0$, there exists a principal minor $M_R$ of $D$ of order $R$ whose rank modulo $P^\lambda$ is $R$, and such that the highest power of $P$ that divides all the $R$-rowed minors of $D$ is exactly the power of $P$ that is contained in $M_R$, or, more precisely, whose elementary exponents are those of $D$ that are less than $\lambda$ and whose elementary ranks are precisely those of $D$. In fact, the $M_{R_k}$ formed by taking the first $R_k$ rows and columns of $D^{(k)}$ is congruent modulo $P^\lambda$ to such a principal minor of $D$ of order $R_k$. From the form of $D^{(k)}$ also follows the fact that the elementary exponent is a monotonically increasing function of the order of the minors.

3. *Criteria for the Classes $Ce_im_iR_k$ and $Ce_im_jnD$.*—It follows from §§ 1 and 2 that the determinant $D$ of a quadratic form, the $e_i$, $r_i$ of $D$ and the rank $R_k=r_1+\ldots+r_k$ of $D$ modulo $P^\lambda$ are invariants. However, these invariants do not completely characterize the classes. We seek criteria for the determination of the $m_i$ of (8) and (9) § 1. Consider the modular form $q_n$ given by (1) and let not all the $a_{ij}$ be zero modulo $P^\lambda$. Under transformations of the type used in § 1, $q_n$ becomes

$$\sum_{s=1}^{k} P^{e_s} \sum_{i,\,j=R_{s-1}+1}^{R_s} A^{(s)}_{ij}x_ix_j, \quad R_s=\sum_{i=1}^{s} r_i, \tag{10}$$

where $e_1<e_2<\ldots.<e_k$ are the distinct elementary exponents of $D$ with respect to $P$ that are less than $\lambda$, and the $r_i$ are the elementary ranks of $D$ with respect to $P$. The determinants $|A_{ij}^{(s)}|$ are prime to $P$, and $R_k$ is the rank modulo $P^\lambda$ of $D$.

Consider first the case $R_k<n$. Let $E_i=r_1e_1+\ldots.+r_ie_i$ and denote the minor $|P^{e_1}A_{ij}^{(1)}|$ of the determinant of (10) by $M_{R_1}$. Then $q_n$ belongs to the class $Ce_im_iR_k$ with $m_1=0$ or 1, according as $(P^{-E_1}M_{R_1})^{\frac{\mu}{2}}\equiv 1$ or $-1 \pmod{P^\lambda}$, where $\mu=\phi(P^\lambda)=P^{\lambda-1}(P-1)$. By §§ 1, 2, $M_{R_1}$ is congruent modulo $P^\lambda$ to an $R_1$-rowed principal minor of $D$ such that $P^{-E_1}M_{R_1}$ is prime to $P$. Let now $M_{R_1}$ denote any such principal minor of $D$. Then, since $q_n$ has one and but one of the canonical forms, we conclude that $q_n$ belongs to the class $Ce_im_iR_k$ with $m_1=0$ or 1 according as $(P^{-E_1}M_{R_1})^{\frac{\mu}{2}}\equiv 1$ or $-1 \pmod{P^\lambda}$. Consider next the minor

$$M_{R_2}\equiv\begin{vmatrix} P^{e_1}A_{11}^{(1)} \ldots. P^{e_1}A_{1,R_1}^{(1)} & 0\ldots\ldots\ldots\ldots 0 \\ \ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ P^{e_1}A_{R_1,1}^{(1)}\ldots. P^{e_1}A_{R_1R_1}^{(1)} & 0\ldots\ldots\ldots\ldots 0 \\ 0\ldots\ldots\ldots 0\ldots\ldots & P^{e_2}A_{R_1+1,R_1+1}^{(2)}\ldots. P^{e_2}A_{R_1+1,R_2}^{(2)} \\ \ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ 0\ldots\ldots\ldots 0\ldots\ldots & P^{e_2}A_{R_2,R_1+1}^{(2)}\ldots\ldots P^{e_2}A_{R_2R_2}^{(2)} \end{vmatrix}.$$

$M_{R_2}$ is an $R_2$-rowed principal minor of the determinant of (10) and is congruent modulo $P^\lambda$ to an $R_2$-rowed principal minor of $D$. Moreover, by §§ 1, 2, $q_n$ belongs to the class $Ce_im_iR_k$ with $m_2=0$ or 1 according as

$$(|A_{ij}^{(2)}|)^{\frac{\mu}{2}}=\left(\frac{P^{-E_2}M_{R_2}}{|A_{ij}^{(1)}|}\right)^{\frac{\mu}{2}}\equiv(|A_{ij}^{(1)}|)^{\frac{\mu}{2}}(P^{-E_2}M_{R_2})^{\frac{\mu}{2}}\equiv 1 \text{ or } -1 \pmod{P^\lambda}.$$

Let now $M_{R_2}$ denote any $R_2$-rowed principal minor of $D$ having an $R_1$-rowed principal minor $M_{R_1}$ such that $P^{-E_2}M_{R_2}$ and $P^{-E_1}M_{R_1}$ are prime to $P$. Then, in view of §§ 1, 2, and the fact that $q_n$ has one and but one of the canonical forms, $q_n$ belongs to the class $Ce_im_iR_k$ with $m_2=0$ or 1 according as

$$(P^{-E_1}M_{R_1})^{\frac{\mu}{2}}(P^{-E_2}M_{R_2})^{\frac{\mu}{2}}\equiv 1 \text{ or } -1 \pmod{P^\lambda}.$$

In general let $M_{R_s}$ be any $R_s$-rowed principal minor of $D$ having an $R_{s-1}$-rowed principal minor $M_{R_{s-1}}$, which in turn has an $R_{s-2}$-rowed principal minor $M_{R_{s-2}}$ and so on to $M_{R_2}$ which has an $R_1$-rowed principal minor $M_{R_1}$ such that $P^{-E_i}M_{R_i}$ $(i=1,\ldots.,s)$ is prime to $P$. Then by a transformation of determinant unity which merely permutes the $x_i$ of (1) we have the principal minors $M_{R_1}$ occupying the first $R_1$ rows and columns of $D$, etc. Then from the form of $D^{(k)}$ of § 2 we have that $q_n$ belongs to the class $Ce_im_iR_k$ with $m_s=0$ or 1 according as

$$\prod_{j=1}^{s}(P^{-E_j}M_{R_j})^{\frac{\mu}{2}}\equiv 1 \text{ or } -1 \pmod{P^\lambda}. \qquad (11)$$

For the case $R_k=n$, $D$ together with (11) for $s=1, \ldots, k-1$ furnish criteria. At the first consideration one would probably be surprised that $D$ may be zero modulo $P^\lambda$ and still $q_n$ belong to class $Ce_i m_j nD$. In fact $D$ may be divisible by a much higher power of $P$ than $P^\lambda$ and still $q_n$ belong to class $Ce_i m_j nD$, since it is not the power of $P$ that divides the minors of $D$ that determine the number of terms in the canonical form, but the elementary exponents of $D$. This phenomenon is what gave rise to the definition of the rank of $D$ modulo $P^\lambda$ of § 2. The rank of $D$ modulo $P^\lambda$ shall be called the rank of the form $q_n$ modulo $P^\lambda$. Two forms $q_n$ and $q'_n$ of rank $n$ are equivalent if and only if

$$e_i=e'_i,\ r_i=r'_i,\ m_j=m'_j \qquad (i=1, \ldots, k;\ j=1, \ldots, k-1)$$

and $P^{-E_k+e_k}D \equiv P^{-E'_k+e'_k}D'$ (mod $P^\lambda$) as is seen by §§ 1, 2.

4. *Invariantive Criteria for the Classes.*—Consider the modular quadratic form (1), and let $e_1<e_2<\ldots<e_h$ be the distinct elementary exponents of $D$ with respect to $P$. Let $\overline{D}$, $\bar{e}_i$, $\bar{r}_i$ and $\bar{m}_i$ be a consistent set of values that define a class $C\bar{e}_i\bar{m}_i\bar{R}_k$ or $C\bar{e}_i\bar{m}_j n\overline{D}$ according as the rank $\bar{R}_k$ modulo $P^\lambda$ of $\overline{D}$ is less than or equal to $n$. For abbreviation set

$$\begin{aligned}
&\mathfrak{R}_i=\sum_{j=1}^{i-1} r_j+\bar{r}_i, \quad \mathfrak{E}_i=\sum_{j=1}^{i-1} r_je_j+\bar{r}_ie_i && (i=1, \ldots, k),\\
&\bar{R}_i=\sum_{j=1}^{i} \bar{r}_j, \qquad \bar{E}_i=\sum_{j=1}^{i} \bar{r}_j\bar{e}_j && (i=1, \ldots, k),\\
&R'_i=\sum_{j=1}^{i-1} r_j+r'_i, \quad E'_i=\sum_{j=1}^{i-1} r_je_j+r'_ie_i && (i=1, \ldots, k;\ \bar{r}_i<r'_i\leqq n-R_{i-1}),\\
&R_i=\sum_{j=1}^{i} r_j, \qquad E_i=\sum_{j=1}^{i} r_je_j && (i=1, \ldots, h).
\end{aligned}$$

Thus $R_h$ and $\bar{R}_k$ are the ranks modulo $P^\lambda$ of $D$ and $\overline{D}$, respectively.

Consider the function*

$$\begin{aligned}
A_{\bar{R}_1}(D) \equiv (P^{e_1-\bar{r}_1})^\mu \{ &(P^{-\mathfrak{E}_1}M^{(1)}_{\mathfrak{R}_1})^{\frac{\mu}{2}}+(P^{-\mathfrak{E}_1}M^{(2)}_{\mathfrak{R}_1})^{\frac{\mu}{2}}[1-(P^{-\mathfrak{E}_1}M^{(1)}_{\mathfrak{R}_1})^\mu]\\
&+\ldots+(P^{-\mathfrak{E}_1}M^{(r)}_{\mathfrak{R}_1})^{\frac{\mu}{2}}\prod_{j=1}^{r-1}[1-(P^{-\mathfrak{E}_1}M^{(j)}_{\mathfrak{R}_1})^\mu]\}\prod_i[1-(P^{-E'_1}M^{(i)}_{R'_1})^\mu] \pmod{P^\lambda}, \quad (12)
\end{aligned}$$

where $M^{(j)}_{\mathfrak{R}_1}$ ranges over the principal minors of $D$ of order $\mathfrak{R}_1=\bar{R}_1$, and $M^{(j)}_{R'_1}$ ranges over the principal minors of $D$ of order $R'_1>\mathfrak{R}_1$. Since $P^{e_1}$ divides all the $a_{ij}$ of $D$, it is evident that there is no term of $A_{\bar{R}_1}(D)$ that has as factor $P$ with a negative exponent. $A_{\bar{R}_1}(D)$ is zero modulo $P^\lambda$, unless $e_1=\bar{e}_1$ and unless at least one of the $P^{-\mathfrak{E}_1}M_{\mathfrak{R}_1}$ is prime to $P$ (since $P\geqq 3$). This implies that $A_{\bar{R}_1}(D)\equiv 0 \pmod{P^\lambda}$ unless the rank modulo $P$ of the determinant $|P^{-e_1}a_{ij}|$ is $\bar{r}_1$. In fact, if $r_1<\bar{r}_1$, none of the $P^{-\mathfrak{E}_1}M_{\mathfrak{R}_1}$ are prime to $P$, while if $r_1>\bar{r}_1$, at least one

* In case $k=1$ and $\lambda>1$, $A_{\bar{R}_1}(D)$ is to have also the final factor of (15).

of the $P^{-E'_1}M_{R'_1}$ is prime to $P$ and the final factor is zero by Fermat's theorem. Thus the value of $A_{\bar{R}_1}(D)$ is zero modulo $P^\lambda$, unless $q_n$ belongs to a class $Ce_im_iR_k$ or $Ce_im_inD$ with $e_1=\bar{e}_1$ and $r_1=\bar{r}_1$, and by (11), § 3, its value modulo $P^\lambda$ is 1 or $-1$ according as $m_1=0$ or 1.

Consider next the function

$$A_{\bar{R}_2}(D)\equiv(P^{e_2-r_2})^\mu\{A_{\bar{R}_1}(M^{(1)}_{\mathfrak{R}_2})\,(P^{-\mathfrak{G}_2}M^{(1)}_{\mathfrak{R}_2})^{\frac{\mu}{2}}+A_{\bar{R}_1}(M^{(2)}_{\mathfrak{R}_2})\,(P^{-\mathfrak{G}_2}M^{(2)}_{\mathfrak{R}_2})^{\frac{\mu}{2}}[1-(P^{-\mathfrak{G}_2}M^{(1)}_{\mathfrak{R}_2})^\mu]$$
$$+\ldots.+A_{\bar{R}_1}(M^{(\sigma)}_{\mathfrak{R}_2})(P^{-\mathfrak{G}_2}M^{(\sigma)}_{\mathfrak{R}_2})^{\frac{\mu}{2}}\prod_{j=1}^{s-1}[1-(P^{-\mathfrak{G}_2}M^{(j)}_{\mathfrak{R}_2})^\mu]\}\prod_{i}[1-P^{-E'_2}M^{(i)}_{R'_2})^\mu]\ (\mathrm{mod}\,P^\lambda),\quad(13)$$

where $M^{(j)}_{\mathfrak{R}_2}$ ranges over the principal minors of $D$ of order $\mathfrak{R}_2$, and $M^{(i)}_{R'_2}$ ranges over the principal minors of $D$ of orders $R'_2>\mathfrak{R}_2$. That the principal minors are divisible by the power of $P$ indicated in (13) follows from the fact that the elementary exponents of $D$ increase monotonically with the order of the minors to which they correspond. In fact, by hypothesis, every minor of order $R_1$ of $D$ is divisible by $P^{r_1e_1}$ while every minor of order $R_1+1$ is divisible by $P^{r_1e_1+e_2}$. Let $\varepsilon$ be the $(R_1+2)$-th elementary exponent of $D$. Then every minor of $D$ of order $R_1+2$ is divisible by $P^{r_1e_1+e_2+\epsilon}$. From the fact that $\varepsilon\geqq e_2$ we see that every minor of $D$ of order $R_1+2$ is divisible by $P^{r_1e_1+2e_2}$. Continuing this we have that every minor of $D$ of order $R_1+\bar{r}_2=\mathfrak{R}_2$ is divisible by $P^{r_1e+r_2e_2}=P^{\mathfrak{G}_2}$. If none of the $P^{-\mathfrak{G}_2}M_{\mathfrak{R}_2}$ are prime to $P$, $A_{\bar{R}_2}(D)\equiv0\ (\mathrm{mod}\,P^\lambda)$. Its value is also zero modulo $P^\lambda$ unless $r_1=\bar{r}_1$, $e_1=\bar{e}_1$ and $e_2=\bar{e}_2$ from the fact that each term carries an $A_{\bar{R}_1}$ function as factor and from the first factor. Thus $A_{\bar{R}_2}(D)$ is zero modulo $P^\lambda$ unless at least one of the $M^{(j)}_{\mathfrak{R}_2}$ is such that $P^{-\mathfrak{G}_2}M_{\mathfrak{R}_2}$ is prime to $P$ and at the same time contains a principal minor $M_{\mathfrak{R}_1}$ such that $P^{-\mathfrak{G}_1}M_{\mathfrak{R}_1}$ is prime to $P$. Let all these conditions be satisfied and take this $P^{-\mathfrak{G}_1}M_{\mathfrak{R}_1}=P^{-\bar{E}_1}M_{\bar{R}_1}$ as the $M_{R_1}$ of §§ 1 and 2. Then we have that $q_n$ is equivalent modulo $P^\lambda$ to a form whose determinant is $D^{(1)}$ of § 2. If $r_2<\bar{r}_2$, all the $\mathfrak{R}_2$-rowed minors of $D^{(1)}$ are divisible by a higher power of $P$ than $P^{\mathfrak{G}_2}$, and hence none of the $P^{-\mathfrak{G}_2}M_{\mathfrak{R}_2}$ of $D$ are prime to $P$. Therefore, $r_2\geqq\bar{r}_2$. If $r_2>\bar{r}_2$, at least one of the $R'_2$-rowed principal minors of $D^{(1)}$ that contains $M_{\mathfrak{R}_1}$ as its leading $R_1$-rowed principal minor is such that $P^{-E'_2}M_{R'_2}$ is prime to $P$, and $A_{\bar{R}_2}(D)$ is zero modulo $P^\lambda$ from its final factor by Fermat's Theorem. Hence $A_{\bar{R}_2}(D)\equiv0\ (\mathrm{mod}\,P^\lambda)$ unless $q_n$ belongs to a class $Ce_im_iR_k$ or $Ce_im_inD$ with $e_1=\bar{e}_1$, $e_2=\bar{e}_2$, $r_1=\bar{r}_1$, $r_2=\bar{r}_2$, and by (11) its value is 1 or $-1$ modulo $P^\lambda$ according as $m_2=0$ or 1. Similarly, we have that the function $(i=1,\ldots.,k-1)$

$$A_{\bar{R}_i}(D)\equiv(P^{e_i-\varepsilon_i})^\mu\{\prod_{j=1}^{i-1}A_{\bar{R}_j}(M^{(1)}_{\mathfrak{R}_i})\,(P^{-\mathfrak{G}_i}M^{(1)}_{\mathfrak{R}_i})^{\frac{\mu}{2}}$$
$$+\prod_{j=1}^{i-1}A_{\bar{R}_j}(M^{(2)}_{\mathfrak{R}_i})\,(P^{-\mathfrak{G}_2}M^{(2)}_{\mathfrak{R}_i})^{\frac{\mu}{2}}[1-(P^{-\mathfrak{G}_i}M^{(1)}_{\mathfrak{R}_i})^\mu]$$
$$+\ldots.+\prod_{j=1}^{i-1}A_{\bar{R}_j}(M^{(i)}_{\mathfrak{R}_i})\,(P^{-\mathfrak{G}_i}M^{(i)}_{\mathfrak{R}_i})^{\frac{\mu}{2}}\prod_{v=1}^{i-1}[1-(P^{-\mathfrak{G}_i}M^{(v)}_{\mathfrak{R}_i})^\mu]\}\prod_{w}[1-(P^{-E'_i}M^{(w)}_{R'_i})^\mu]$$
$$(\mathrm{mod}\,P^\lambda),\quad(14)$$

where $M^{(v)}_{\mathfrak{R}_i}$ ranges over the principal minors of $D$ of order $\mathfrak{R}_i$, and $M^{(w)}_{R'_i}$ ranges over the principal minors of $D$ of order $R'_i > \mathfrak{R}_i$, has the value zero unless $q_n$ belongs to a class $Ce_i m_i R_k$ or to a class $Ce_i m_j nD$ with $e_j = \bar{e}_j$, $r_j = \bar{r}_j$, and that for such forms its value is 1 or $-1$ modulo $P^\lambda$ according as $m_i = 0$ or 1. When $\bar{R}_k < n$, we have

$$\begin{aligned} A_{\bar{R}_k}(D) \equiv (P^{e_k - \bar{e}_k})^\mu \Big\{ & \prod_{i=1}^{k-1} A_{\bar{R}_i}(M^{(1)}_{\mathfrak{R}_k}) \, (P^{-\mathfrak{E}_k} M^{(1)}_{\mathfrak{R}_k})^{\frac{\mu}{2}} \\ & + \prod_{i=1}^{k-1} A_{\bar{R}_i}(M^{(2)}_{\mathfrak{R}_k}) \, (P^{-\mathfrak{E}_k} M^{(2)}_{\mathfrak{R}_k})^{\frac{\mu}{2}} [1 - (P^{-\mathfrak{E}_k} M^{(1)}_{\mathfrak{R}_k})^\mu] \\ & + \ldots + \prod_{i=1}^{k-1} A_{\bar{R}_i}(M^{(t)}_{\mathfrak{R}_k}) \, (P^{-\mathfrak{E}_k} M^{(t)}_{\mathfrak{R}_k})^{\frac{\mu}{2}} \prod_{j=1}^{t-1} [1 - (P^{-\mathfrak{E}_k} M^{(j)}_{\mathfrak{R}_k})^\mu] \Big\} \\ & \prod_v [1 - (P^{-E'_k} M^{(v)}_{R'_k})^\mu] \prod_w [1 - (P^{-(E_k + e_{k+1})} d^{(w)}_{R_k+1})^\mu] \pmod{P^\lambda}, \end{aligned} \tag{15}$$

where $M^{(j)}_{\mathfrak{R}_k}$ ranges over the principal minors of $D$ of order $\mathfrak{R}_k$, $M^{(v)}_{R'_k}$ ranges over those of order $R'_k > \mathfrak{R}_k$, $d^{(w)}_{R_k+1}$ ranges over the minors of $D$ of order $R_k + 1$, and $e_{k+1}$ is the $(R_k+1)$-th elementary exponent of $D$. In case $e_{k+1} \geqq \lambda$, define $P^{-(E_k + e_{k+1})} d^{(w)}_{R_k+1}$ to be zero modulo $P^\lambda$. Then $A_{\bar{R}_k}(D)$ has the value zero unless $e_i = \bar{e}_i$, $r_i = \bar{r}_i$ $(i = 1, \ldots, k)$ and $e_{k+1} \geqq \lambda$, whence $R_k = R_k = \bar{R}_k$. Hence $A_{\bar{R}_k}(D) \equiv 0 \pmod{P^\lambda}$ unless $q_n$ belongs to a class $Ce_i m_i R_k$ with $e_i = \bar{e}_i$ and $r_i = \bar{r}_i$ $(i = 1, \ldots, k)$, and for such forms its value is 1 or $-1$ according as $m_k = 0$ or 1. When $\bar{R}_k = n$ we have

$$\begin{aligned} A_n(D) \equiv (P^{e_k - \bar{e}_k})^\mu (P^{-E_k} D)^\mu \{1 - [(P^{-E_k + e_k} D - P^{-\bar{E}_k + \bar{e}_k} \bar{D}) P^{-q}]^\mu \} \Big\{ & \prod_{i=1}^{k-1} A_{\bar{R}_i}(D) \\ & \pmod{P^\lambda}, \end{aligned} \tag{16}$$

where $P^q$ is the highest power of $P$ that divides $P^{-E_k + e_k} D - P^{-\bar{E}_k + \bar{e}_k} \bar{D}$. In case $q \geqq \lambda$, define $P^{-q}(P^{-E_k + e_k} D - P^{-\bar{E}_k + \bar{e}_k} \bar{D})$ to be zero modulo $P^\lambda$. Then the value of $A_n(D)$ is zero modulo $P^\lambda$ unless $e_i = \bar{e}_i$, $r_i = \bar{r}_i$ $(i = 1, \ldots, k)$ and $P^{-E_k + e_k} D \equiv P^{-\bar{E}_k + \bar{e}_k} \bar{D} \pmod{P^\lambda}$. The function is also zero unless $P^{-E_k} D$ is prime to $P$, *i. e.*, unless the rank modulo $P^\lambda$ of $D$ is $R_k$. Hence $A_n(D)$ is zero modulo $P^\lambda$ unless $q_n$ belongs to a class $Ce_i m_j nD$ with $e_i = \bar{e}_i$, $r_i = \bar{r}_i$ $(i = 1, \ldots, k)$ and its value is 1 modulo $P^\lambda$ for all such forms.

Finally, define $P^{-e_1} a_{ij}$ to be zero modulo $P^\lambda$ when $e_1 \geqq \lambda$. Then

$$I \equiv \Pi [1 - (P^{-e_1} a_{ij})^\mu] \pmod{P^\lambda} \qquad (i, j = 1, \ldots, n;\ i \leqq j) \tag{17}$$

has the value zero modulo $P^\lambda$ unless $q_n$ belongs to the class $C_0$ and the value 1 for such a form. The functions $A_{\bar{R}_i}(D)$, $A_n(D)$ and $I$ are modular invariants that completely characterize the classes of modular quadratic forms modulo $P^\lambda$.

5. *Characteristic Modular Invariants.*—An invariant $\phi$ that has the value 1 for all forms of one class, and the value zero for forms of any other

class is called a characteristic invariant. In case such a $\phi$ is a modular invariant it is called a characteristic modular invariant. For example, $I$ is a characteristic invariant for the class $C_0$.

Let $\bar{e}_i, \bar{r}_i, \overline{m}_i$ $(i=1, \ldots, k)$ be a set of consistent values that define the class $C\bar{e}_i\overline{m}_i\bar{R}_k$. Among the integers $1, \ldots, k$ a certain number $s_1$ of them will correspond to $m$'s that are zero. The remaining $s_2$ of them will correspond to $m$'s that are unity. Call the first set $\sigma_1$, and the second, $\sigma_2$, and consider the function

$$A_{\bar{R}_k\sigma_1\sigma_2} \equiv \frac{1}{2^{s_1+s_2}} \prod_i [(A_{\bar{R}_i}(D))^2 + A_{\bar{R}_i}(D)] \prod_j [(A_{\bar{R}_j}(D))^2 - A_{\bar{R}_j}(D)] \pmod{P^\lambda}, \quad (18)$$

where $i$ ranges over $\sigma_1$, and $j$ ranges over $\sigma_2$. This function has the value 1 * for all forms of class $C\bar{e}_i\overline{m}_i\bar{R}_k$ and the value zero for all other forms. Hence $A_{\bar{R}_k\sigma_1\sigma_2}$ is a characteristic modular invariant of $q_n$.

Next let $\bar{e}_i, \bar{r}_i$ $(i=1, \ldots, k)$, $\overline{m}_j$ $(j=1, \ldots, k-1)$ and $\overline{D}$ be a consistent set of values of these quantities that define the class $C\bar{e}_i\overline{m}_jn\overline{D}$; thus $\bar{R}_k=n$. Separate the integers $1, \ldots, k-1$ into sets $\sigma_1$ and $\sigma_2$ composed of $s_1$ and $s_2$ elements, respectively, such that those of $\sigma_1$ correspond to the $m$'s that are zero, while those of $\sigma_2$ correspond to the $m$'s that are unity. Then the function

$$A_{n\sigma_1\sigma_2} \equiv \frac{1}{2^{s_1+s_2}} \prod_i [(A_{\bar{R}_i}(D))^2 + A_{\bar{R}_i}(D)] \prod_j [(A_{\bar{R}_j}(D))^2 - A_{\bar{R}_j}(D)] A_n(D) \pmod{P}, \quad (19)$$

where $i$ ranges over $\sigma_1$ and $j$ ranges over $\sigma_2$, has the value 1 for all forms of class $C\bar{e}_i\overline{m}_jn\overline{D}$ and the value zero for all other forms.

Hence the characteristic invariants $A_{\bar{R}_k\sigma_1\sigma_2}$, $A_{n\sigma_1\sigma_2}$, and $I$ completely characterize the classes of modular quadratic forms modulo $P^\lambda$.

For the case $\lambda=1$, $A_{\bar{R}_0}(D)$ and $A_{\bar{R}_k\sigma_1\sigma_2}$ become, respectively, the invariants $A_r$ and $I_{r,\pm 1}$ given by Professor Dickson in his Madison Colloquium lectures, pp. 11, 13. The function $A_{n\sigma_1\sigma_2}$ is for this case a characteristic invariant of his class $C_{nD}$, while $I$ in this case is replaced by the simple form $I=\Pi(1-a_{ij}{}^\mu)$, as given *loc. cit.*, p. 11. These are the only ones that enter in this case, since the only set of integers $e_i, m_i, r_i$ are $0, r_1, m_1$. Thus, for this case the invariants given above are all polynomial modular invariants. This may also happen for the case $\lambda>1$, but would obviously be a very special case.

6. *Number of Linearly Independent Modular Invariants of $q_n$.*—For convenience denote the classes of modular quadratic forms modulo $P^\lambda$ by $C_0, C_1, C_2, \ldots$ and the corresponding characteristic invariants by

* In case either $\sigma_1$ or $\sigma_2$ is an empty set, the corresponding product factors of (18) is defined to be unity. Similarly in (19).

$I_0, I_1, I_2, \cdots$. Since any modular invariant $I$ of $q_n$ takes certain values $v_0, v_1, v_2, \ldots$ for the respective classes $C_0, C_1, C_2, \ldots$ we have

$$I \equiv v_0 I_0 + v_1 I_1 + v_2 I_2 + \ldots \pmod{P^\lambda}.$$

Hence, any modular invariant is congruent to a linear homogeneous function of the characteristic invariants. Moreover, the number of linearly independent modular invariants of the quadratic form $q_n$ modulo $P^\lambda$ equals the number of classes.

## II. Polynomial Modular Invariants of a Binary Quadratic Form.

7. *Invariants for a Prime Power Modulus $P^\lambda$.*—Consider the form

$$f = a_0 x^2 + a_1 xy + a_2 y^2, \tag{1}$$

where the $a_i$ are integers taken modulo $P^\lambda$. The transformations *

$$\begin{aligned} R&: x = x' + Ty', \quad y = y', \\ S&: x = x', \quad y = ky', \quad (k \text{ prime to } P) \\ Q&: x = y', \quad y = -x', \end{aligned}$$

generate the group of all linear homogeneous transformations whose determinant is prime to $P$ and coefficients are integers modulo $P^\lambda$. Transformations $R, S, Q$ give the respective replacements

$$a_0' = a_0, \quad a_1' = a_1 + 2a_0 T, \quad a_2' = a_2 + a_1 T + a_0 T^2. \tag{2}$$

$$a_0' = a_0, \quad a_1' = k a_1, \quad a_2' = k^2 a_2. \tag{3}$$

$$a_0' = a_2, \quad a_1' = -a_1, \quad a_2' = a_0. \tag{4}$$

Theorem 1. *The form $f$ has the absolute invariant modulo $P^\lambda$*

$$H = \prod_{i=0}^{2} (a_i^\mu - 1) \qquad \mu = \phi(P^\lambda) = P^{\lambda-1}(P-1).$$

Evidently replacements (3) and (4) leave $H$ unaltered. It remains to show that $H$ is unaltered by replacement (2). This is evident if $a_0$ is prime to $P$, since then $a_0^\mu - 1 \equiv 0 \pmod{P^\lambda}$. Hence let $a_0$ be divisible by $P$. Then $a_1'$ is of the form $a_1 + Pq$ and, by induction on $\lambda$,

$$(a_1 + Pq)^{P^{\lambda-1}} \equiv a_1^{P^{\lambda-1}} \pmod{P^\lambda},$$

whence $a_1'^\mu \equiv a_1^\mu$. Hence $H' \equiv A(a_2'^\mu - 1)$, where

$$A = (a_0^\mu - 1)(a_1^\mu - 1).$$

Thus $H' \equiv H$ if either $a_0$ or $a_1$ is prime to $P$. In the contrary case, $a_2 = a_2 + Pq$ and $a_2'^\mu \equiv a_2^\mu$ as before, whence $H' \equiv H$ in all cases.

---

* Cf. C. Jordan, "Traité des Substitutions," p. 93.

The same method leads to

THEOREM 2. *The form f has the absolute invariants modulo* $2^\lambda$

$$I=a_1^\mu=a_1^{2^{\lambda-1}}, \quad Q=a_0^\mu a_1^\mu a_2^\mu.$$

8. *Fundamental System of Invariants Modulo* 4.

THEOREM 3. *Necessary and sufficient conditions that*

$$\alpha+\beta T+\gamma T^2+\delta T^3\equiv 0 \pmod 4$$

*for all integral values of* $T$ *are*

$$\alpha\equiv 0, \quad 2\beta\equiv 2\gamma\equiv\beta+\gamma+\delta\equiv 0 \pmod 4.$$

The general invariants of § 7 become

$$H=\prod_{i=0}^{2}(a_i^3-1), \quad I=a_1^3, \quad Q=a_0^3a_1^3a_2^3.$$

A useful combination of these invariants is

$$S=P-Q-I+1=a_0^2+a_2^2-a_0^2a_2^2-a_0^2a_1^2-a_1^2a_2^2.$$

THEOREM 4. *The form f has the absolute invariants* *

$$\begin{aligned}
K&\equiv a_1+a_1^3+2a_0a_2,\\
J&\equiv 2a_0+2a_2+a_0a_1+a_0a_1^2+a_1a_2+a_1a_2^2+a_0a_1a_2+a_0a_1^2a_2,\\
E&\equiv a_0a_2+a_0^2a_2^2+a_0a_2(a_1+a_1^2+a_1^3)\\
&\equiv a_0^2a_2+a_0a_2^2+a_0^2a_2^2-a_0^2a_2^2+a_0a_1a_2^2+a_0^2a_1^2a_2+a_0^2a_1^2a_2^2 \pmod 4.
\end{aligned}$$

The following identical congruences are of use in simplifying the discussion given below for the general invariant.

$$U\equiv(a_1+a_1^2)(a_2+a_2^2)\equiv 0, \quad V\equiv(a_0+a_0^2)(a_1+a_1^2)\equiv 0, \quad L\equiv(a_0+a_0^2)(a_2+a_2^2)\equiv 0,$$

$$Q_1=3Q\equiv a_0^2a_1^2a_2^2+a_0^2a_1^2a_2^2+a_0^2a_1^2a_2^2, \quad Q_2=3Q\equiv a_0^2a_1^2a_2+a_0^2a_1^2a_2+a_0^2a_1^2a_2^2,$$

$$M\equiv a_0a_1a_2^2+a_0^2a_1a_2^2+a_0a_1^2a_2+a_0^2a_1^2a_2\equiv 4Q\equiv 0,$$

$$N\equiv a_0a_1a_2^2+a_0^2a_1a_2^2+a_0a_1^2a_2+a_0^2a_1^2a_2\equiv 4Q\equiv 0.$$

In view of the identical congruence $x^4\equiv x^2 \pmod 4$, we may assume that the exponent of each $a_i$ in an invariant of $f$ does not exceed 3. Hence, we may denote any invariant $\phi$ by

$$\phi\equiv\sum_{i,j=0}^{3}A_{ij}a_1^ia_2^j, \quad A_{ij}=\alpha_{ij}+\beta_{ij}a_0+\gamma_{ij}a_0^2+\delta_{ij}a_0^3, \tag{5}$$

where $\alpha_{ij}$, etc., are constants. The difference

$$\phi-(A_{11}+A_{12}a_2+A_{31}a_1+A_{33}a_1a_2)U$$

has

$$A_{11}\equiv A_{12}\equiv A_{31}\equiv A_{33}\equiv 0.$$

---

* $K$, $J$ and $E$ were discovered by carrying through for special cases the discussion made below for finding the general invariant; they were verified to be invariant with respect to the generators $R, S, Q$.

Hence, we may assume that in the initial $\phi$ these quantities are zero modulo 4. Similarly, by considering in turn

$$\phi-[\beta_{01}+(\gamma_{01}-\beta_{01})a_0]L-(\delta_{01}-\gamma_{01}+\beta_{01})E,\quad \phi-\alpha_{10}K-[\beta_{10}+(\gamma_{10}-\beta_{10})a_0]V,$$
$$\phi-[\beta_{30}+(\gamma_{30}-\beta_{30})a_0]a_1V,\qquad \phi-[\beta_{03}+(\gamma_{03}-\beta_{03})a_0]a_2L,$$

we may assume that

$$A_{01}\equiv\alpha_{01},\quad A_{10}\equiv\delta_{10}a_0^3,\quad A_{30}\equiv\alpha_{30}+\delta_{30}a_0^3,\quad A_{03}\equiv\alpha_{03}+\delta_{03}a_0^3.$$

Then by employing in turn

$$\phi-\beta_{21}M-\gamma_{21}Q_2,\quad \phi-\beta_{32}N-\gamma_{32}Q_1,\quad \phi-\alpha_{12}J-\gamma_{12}Q_2,\quad \phi-\alpha_{20}I-\gamma_{22}Q+\alpha_{22}S,$$

we may take

$$A_{21}\equiv\alpha_{21}+\delta_{21}a_0^3,\quad A_{32}\equiv\alpha_{32}+\delta_{32}a_0^3,\quad A_{12}\equiv\beta_{12}a_0+\delta_{12}a_0^3,\quad \alpha_{20}=\alpha_{22}=\gamma_{22}=0.$$

At no step have any of the quantities previously taken to be zero been disturbed.

Subjecting the simplified $\phi$ to replacement (2) we get

$$\phi'\equiv\phi+\beta T+\gamma T^2+\delta T^3,$$

where

$$\begin{aligned}
\beta\equiv{}&2A_{10}a_0+2A_{12}a_0+2A_{02}a_0a_2+2A_{12}a_0a_2+(A_{01}+2A_{02}a_0+2A_{22}a_0+2A_{30}a_0\\
&+2A_{32}a_0+2A_{02}a_2+2A_{03}a_0a_2+2A_{12}a_2+2A_{12}a_0a_2+2A_{22}a_2+2A_{22}a_0a_2\\
&+2A_{23}a_0a_2+2A_{32}a_2+3A_{03}a_2^2)a_1+(A_{21}+3A_{23}a_2^2)a_1^3,\\
\gamma\equiv{}&A_{01}a_0+A_{02}a_0^2+A_{03}a_0^3+3A_{03}a_0a_2^2+3A_{03}a_0^2a_2+A_{12}a_0^2a_1+(A_{02}+3A_{03}a_2+A_{21}a_0\\
&+3A_{03}a_0+A_{23}+A_{22}a_0^2+3A_{22}a_0a_2^2+3A_{23}a_2+3A_{23}a_0^2a_2+3A_{23}a_0+A_{23}a_0^3)a_1^2\\
&+(A_{12}+A_{32}+A_{32}a_0^2)a_1^3,\\
\delta\equiv{}&3A_{03}a_0^2a_1+(A_{03}+A_{23}+3A_{23}a_0^2)a_1^3.
\end{aligned}$$

By Theorem 3, necessary and sufficient conditions that $\phi'-\phi\equiv0$ for all integral values of $T$ are $2\beta\equiv2\gamma\equiv\beta+\gamma+\delta\equiv0$. From the form of $A_{10}$, $A_{12}$ and $A_{22}$ we see that

$$2(A_{12}+A_{12}a_0)\equiv0,\quad 2(A_{22}+A_{22}a_0)\equiv0,\quad 2(A_{10}+A_{10}a_0)\equiv0. \tag{6}$$

From $2\beta\equiv2(A_{01}+A_{21})a_1+2(A_{03}+A_{23})a_1a_2$, we have

$$2(A_{01}+A_{21})\equiv0,\quad 2(A_{03}+A_{23})\equiv0. \tag{7}$$

Next,

$$2\gamma\equiv2(A_{01}+A_{02}+A_{03})a_0+2[A_{02}+A_{22}+A_{12}+A_{32}+a_0(A_{12}+A_{21}+A_{03}+A_{22}+A_{32})]a_1.$$

Hence, in view of (7), and (6),

$$2(A_{01}+A_{02}+A_{03})a_0\equiv0,\quad 2(A_{02}+A_{32})(1+a_0)\equiv0. \tag{8}$$